## REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-31 are pending in the application. The Examiner additionally stated that claims 1-31 are rejected. By this communication, claims 1, 18, 25-26, and 31 are amended. Hence, claims 1-31 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

**In the Specification**

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

**In the Claims**

**Rejections Under 35 U.S.C. §103(a)**

The Examiner rejected claims 1-31 under 35 U.S.C. 103(a) as being unpatentable over Yup et al., US2002/0191784, (hereinafter, "Yup") in view of Dhir et al., US2005/0084076 (hereinafter, "Dhir"). Applicant respectfully traverses the Examiner's rejections.

As per claim 1, the Examiner noted that Yup disclose an apparatus for performing cryptographic operations, comprising:

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes one of a plurality of data block sizes (noting that AES block cipher can be performed on 128-bit, 192-bit or 256-bit blocks) [page 4, paragraph 0045]; and
- execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, said execution logic comprising a block size controller (key expansion block), configured to employ

said one of a plurality of data block sizes during execution of said one of the cryptographic operations [page 3, paragraph 0028].

The Examiner conceded that Yup does not explicitly disclose performing these instructions on a microprocessor based platform.

Nonetheless, the Examiner opined that Dhir discloses a similar apparatus and further discloses performing cryptographic instructions (i.e., program instructions) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform(i.e., FPGA) [page 5, paragraph 0051].

Therefore, the Examiner concluded that it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a microprocessor based platform or any other platform in order to meet particular design requirements.

The Examiner stated that Applicant argued that Yup does not disclose cryptographic instructions. However, the Examiner disagreed and submitted that while the exact term "cryptographic instructions" is not disclosed, Yup does in fact teach cryptographic instructions(i.e., finite state machine controllers which controls the operation of the remaining portions of the circuit) [page 3, paragraph 0025].

Furthermore, the Examiner noted that Applicant argued that Yup does not disclose cryptographic instructions received by a microprocessor, yet the Examiner submitted that this is moot in view of the new ground of rejection.

Moreover, the Examiner stated that Applicant argued that Yup does not disclose execution logic coupled to a cryptographic instruction, configured to prescribe a plurality of data block sizes. However, the Examiner disagreed and submitted that Yup does in fact disclose these features (i.e., finite state machine controllers which control the operation of the remaining portions of the circuit, such as the data blocks of which can support block lengths of 128, 192, and 256 bits) [page 3, paragraphs 0026 & 0028 & 0039].

In reply, Applicant respectfully disagrees with the Examiner's characterizations of both Yup and Dhir vis-à-vis that subject matter which is recited in claim 1. To aid in the following analysis, claim 1, as amended herein, is repeated below.

1. An apparatus for performing cryptographic operations, comprising:

fetch logic, disposed within a microprocessor, configured to receive a cryptographic instruction as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes one of a plurality of data block sizes; and

execution logic, disposed within said microprocessor and operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, said execution logic comprising:

a block size controller, configured to employ said one of a plurality of data block sizes during execution of said one of the cryptographic operations.

Applicant respectfully asserts, again, that Yup does not teach a cryptographic instruction. In fact, Applicant has been careful to search Yup and reports that the term "cryptographic instruction" cannot be found. In reply to the Examiner's point that Yup does in fact teach cryptographic instructions (i.e., finite state machine controllers which controls the operation of the remaining portions of the circuit) [page 3, paragraph 0025], Applicant responds that the instant disclosure clearly teaches the meaning of an "instruction" such that it is quite distinct from a finite state machine controller as is taught by Yup in the cited section. The instant disclosure teaches that an instruction, such as the cryptographic instruction recited in claim 1, is part of an application program. Clearly, a finite state machine controller is not part of an application program. As one skilled in the art will appreciate, a application program's instructions are fetched from memory for execution by a microprocessor. To this end, Applicant has amended claim 1 to clearly recite fetch logic, *disposed within a microprocessor,* configured to receive a cryptographic

instruction as part of an instruction flow executing on said microprocessor. These features of the present invention are not taught or suggested by Yup.

In contrast, Yup teaches "A circuit includes a single circuit portion for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels. The circuit portion includes a circuit for individually generating, on the fly, the round keys used during each round of the AES block cipher algorithm. The circuit portion also includes shared logic circuits that implement the transformations used to encrypt and decrypt data blocks according to the AES block cipher. The single circuit portion encrypts or decrypts data blocks from each of the plurality of system channels in turn, in round-robin fashion. The circuit portion also includes a circuit for determining S-box values for the AES block cipher algorithm. The circuit additionally implements an efficient method for generating round keys on the fly for the AES block cipher decryption process. (Abstract)

Without a doubt, Yup. teaches a circuit for implementing the AES block cipher algorithm in a system having a plurality of channels. This is somewhat analogous to prior art stand-alone cryptographic processing units, the problems of which the present inventors have noted and for which the present invention is provided to overcome. Yet, Yup is utterly silent with regard to how the invention is commanded to process data blocks other than to present a plurality of input registers 102 and associated control signals 103 that are coupled to a corresponding plurality of "system channels."

One skilled will appreciate that this type of configuration is cumbersome in that to provide for encryption and/or decryption of data, a processor must provide for communication with Yup's device via some system channel mechanism.

In stark contrast, claim 1 recites a cryptographic instruction that is fetched from memory by a microprocessor as part of an instruction flow executing on said microprocessor. The claim continues to recite how the cryptographic instruction prescribes one of a plurality of data block sizes. Yup does not teach or suggest an instruction that provides for the foregoing limitations. The claim also recites execution logic that is within the microprocessor as well and that is operatively coupled to said cryptographic instruction,

configured to execute said one of the cryptographic operations, said execution logic comprising: block size controller, configured to employ said one of a plurality of data block sizes during execution of said one of the cryptographic operations. Although Yup teach a key expansion block, as the Examiner suggests, such a block is not operatively coupled to a cryptographic instruction that is fetched from memory as part of an instruction flow, for Yup is silent in this regard.

In reply to the Examiner's concession that Yup does not explicitly disclose performing these instructions on a microprocessor based platform, Applicant agrees. And moreover, Applicant specifically notes that claim 1 does not recite a "microprocessor based platform" but rather a "microprocessor."

Consequently, in reply to the Examiner's statement that that Dhir discloses a similar apparatus and further discloses performing cryptographic instructions (i.e., program instructions) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform (i.e., FPGA), Applicant wishes to make several points. First, as noted above, claim 1 specifically recites a microprocessor, not a microprocessor based platform. It is furthermore asserted that a microprocessor is clearly disclosed within the instant specification and drawings and is quite distinct from a microprocessor based platform, which one skilled in the art will appreciate to comprise, for example, one or more microprocessors, memory, coprocessors, I/O, operator interface, etc. And while the hardware to perform cryptography is presently known to be disposed as a coprocessor, it is respectfully asserted that there is no implementation of a microprocessor that includes such capability.

Secondly, Applicant respectfully disagrees with the Examiner's characterization of Dhir's invention as a microprocessor based platform. Applicant submits that one skilled in the art would characterize Dhir's invention as a field programmable gate array (FPGA) is that is coupled to memory having programming instructions for configuring the FPGA with a medium access layer selected from more than one type of medium access layers. [Abstract – an FPGA is not a microprocessor, nor is it a microprocessor based platform.]

Applicant further submits that a more correct characterization of Dhir's invention would be a FPGA-based platform.

Applicant has been careful to search Dhir and finds that a microprocessor is only mentioned twice and it is noted that fixed logic circuit 32 may be a microprocessor, which is provided to replace a set of configurable logic blocks 80, a set of memory blocks 90, and/or a set of multipliers 92, as are found in the X4000E family of field programmable gate arrays and/or the Virtex-II field programmable gate arrays. [paragraphs [0033] and [0037]]. Certainly Dhir does not teach, nor does he suggest, a microprocessor as is disclosed in the instant application and which is recited in claim 1. All Dhir teaches is that one may replace fixed logic 32 with a microprocessor. Dhir certainly does not teach a microprocessor that fetches and executes cryptographic instructions as part of an instruction flow (i.e., an application program). Applicant provides an example of a microprocessor in the instant disclosure as an x86-compatible microprocessor. This is obviously not what is taught by either Yup or Dhir, nor can it be derived from a combination of the two references.

Again, Applicant stresses that the approaches of both Yup and Dhir are techniques employed by hardware *external to a microprocessor,* the disadvantages and limitations of which Applicant notes within the instant application. The apparatus of claim 1, on the other hand, performs cryptographic operations *within a microprocessor, responsive to a cryptographic instruction fetched from memory,* which is advantageous in one aspect in that an instruction is provided for use by a programmer to instruct the microprocessor to perform one of a plurality of cryptographic operations.

Based upon the above arguments, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

With respect to claims 2-17, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup, Dhir, or a combination of the two references Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-17.

As per claim 18, the Examiner noted that Yup disclose an apparatus for performing cryptographic operations, comprising:

- a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes a block size to be employed when executing said one of the cryptographic operations (AES block cipher can be performed on 128-bit, 192-bit, or 256-bit blocks) [page 4, paragraph 0045]; and
- block size logic (key expansion block), operatively coupled within said cryptography unit, configured to direct said device to employ said block size when performing said one of the cryptographic operations [page 3, paragraph 0028].

The Examiner stated that Yup does not explicitly disclose performing these instructions on a microprocessor based platform, but that Dhir discloses a similar apparatus and further discloses performing cryptographic instructions(i.e., program instructions) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform(i.e., FPGA) [page 5, paragraph 0051].

The Examiner therefore concluded that it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a microprocessor based platform or any other platform in order to meet particular design requirements.

Applicant respectfully disagrees with the Examiner's arguments provided above and directs attention to the arguments submitted in traversal of the rejection of claim 1. In summary, Yup's invention is a stand-alone unit, not part of a microprocessor. As such, it does not execute an instruction flow. And furthermore, the instruction flow does not provide a cryptographic instruction that prescribes, *inter alia*, a block size to be employed when executing said one of the cryptographic operations.

In addition, Dhir's invention is a field programmable gate array (FPGA) is that is coupled to memory having programming instructions for configuring the FPGA with a medium access layer selected from more than one type of medium access layers. Dhir's FPGA is not a microprocessor, nor does it teach or suggest fetch logic within a microprocessor for fetching a cryptographic instruction from memory.

In view of the above arguments, it is respectfully requested that the rejection of claim 18 be withdrawn.

With respect to claims 19-24 these claims depend from claim 18 and add further limitations that are neither anticipated nor made obvious by Yup, Dhir, or a combination of the references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 19-24.

As per claim 25, the Examiner noted that Yup disclose a method for performing cryptographic operations in a device, the method comprising:

- receiving a cryptographic instruction that prescribes employment of a particular block size for employment during execution of one of a plurality of cryptographic operations (AES block cipher can be performed on 128-bit, 192-bit, or 256-bit blocks) [page 4, paragraph 0045];
- and employing the data block size(key expansion block uses "nb", the block size, to generate a round key) when executing the one of the cryptographic operations [page 3, paragraphs 0028-0035].

The Examiner stated that Yup, nonetheless, does not explicitly disclose performing these instructions on a microprocessor based platform, but that Dhir discloses a similar method and further discloses performing cryptographic instructions (i.e., program instructions) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform (i.e., FPGA) [page 5, paragraph 0051].

The Examiner therefore concluded that it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a microprocessor based platform or any other platform in order to meet particular design requirements.

Applicant respectfully disagrees with the points asserted above and directs the Examiner's attention to the arguments submitted in traversal of the rejections of claims 1 and 20. Claim 25 recites, among other elements and limitations, within a microprocessor, fetching a cryptographic instruction—not instructions, plural—from memory that prescribes a cryptographic key size for employment during execution of one of a plurality of cryptographic operations. As noted earlier, Yup does not teach a microprocessor, nor it is taught that the microprocessor receives a cryptographic instruction that prescribes data block size for employment during execution of one of a plurality of cryptographic operations. This is because Yup teaches a stand-alone AES unit that is fed data from system channels. In addition, Dhir teaches using FPGAs to configure a MAC layer device on a wireless LAN. Neither Yup nor Dhir teach or suggest fetching a cryptographic instruction from memory that prescribes a cryptographic key size for employment during execution of one of a plurality of cryptographic operations, and executing the cryptographic instruction while employing the prescribed data block size—*in a microprocessor.*

Accordingly, it is respectfully requested that the rejection of claim 25 be withdrawn.

With respect to claims 26-31, these claims depend from claim 25 and add further limitations that are neither anticipated nor made obvious by Yup, Dhir, or a combination of the cited references Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 26-31.

## CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-31 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
**HUFFMAN PATENT GROUP, LLC**

/Richard K. Huffman/

By: _____

**RICHARD K. HUFFMAN, P.E.**
Registration No. 41,082
Tel: (719) 575-9998

10/24/2001

Date: _____